The Internet, New Media, and the Evolution of Insurgency

Steven Metz

Introduction

Insurgency, like war, has an enduring nature and a changing character. It remains a strategy entailing violence used by the weak and desperate against a power system.[1] Often (but not always), this pits a nonstate or proto-state organization against a state. Out of weakness, the organization using a strategy of insurgency attempts to shift the focus of conflict away from domains where the state or other power structure is particularly strong, particularly the conventional military. Insurgents seek to make domains decisive where morale and other psychological characteristics matter more than tangible power, recognizing these characteristics even the odds to a certain extent. The enduring nature of insurgency includes three core functions: an insurgency must survive, it must strengthen itself, and it must weaken the power structure or state.

How an insurgency accomplishes these three objectives constitutes the changing character of the phenomenon. Throughout the long history of insurgency there have been multiple types or models. Today, three exist in various parts of the world. One is the *proto-state*. Derived from the Maoist movements of the twentieth century, this is often considered the gold standard for any insurgency. In this model, an insurgency weakens the state through guerrilla attacks, terrorism, subversion, and psychological operations while it simultaneously serves the functions of the state in areas it controls. By demonstrating that it can provide better services than the existing state, it hopes to win support and eventually replace the existing government. This type of insurgency was particularly effective in peasant societies where active popular support mattered greatly; hence, the insurgents and the state competed for that support. In the classic Maoist method, final victory comes when the insurgency is the equal of the state politically, militarily, and economically. The organizations created

Steven Metz is research professor and chairman of the Regional Strategy Department at the US Army War College Strategic Studies Institute (SSI). He has been at SSI since 1993, previously serving as Director of Research and Henry L. Stimson Professor of Military Studies. Dr. Metz is also a member of the RAND Insurgency Board and writes a weekly column on defense and security for World Politics Review. He is the author of Iraq and the Evolution of American Strategy ***(2008).***

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2012		**00-00-2012 to 00-00-2012**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
The Internet, New Media, and the Evolution of Insurgency	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **U.S. Army War College,ATTN: Parameters,47 Ashburn Drive,Carlisle,PA,17013-5010**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**11**	

by Mao and his best student—Ho Chi Minh—ultimately won conventional military victories over the Chinese and Vietnamese and were immediately prepared to assume the role of the state.

The second model—and one which is more controversial among insurgency theorists—is *nonpolitical*. Rather than seeking to replace the state, this type of insurgent simply wants to weaken the state sufficiently to be free of its control. Normally, it is the insurgent's intent to practice some form of organized criminal activity. Like organized crime everywhere, these insurgents seek passivity more than active popular support. The methods of such insurgents, though, are quite similar to the politically focused insurgent. Mexico today is one example of this while some other insurgencies that began life as proto-state insurgencies eventually devolved into nonpolitical or what might be called commercial insurgencies.[2] Examples of these include the Fuerzas Armadas Revolucionarias de Colombia (FARC) in Colombia, Shining Path in Peru, and a number of African movements.

The third model consists of insurgencies that hope to replace the state but, because they are unable to control significant territory, approach the goal of destroying the state and replacing it in a sequential rather than simultaneous manner. Their initial focus is destruction. Again, active support is less important than passivity. They use a dispersed, networked organization and rely on the swarming method of attacks dominated by terrorism rather than guerrilla or conventional military operations. To augment their ability to survive and increase their own strength, they develop an important transnational dimension. Since traditional, Maoist style insurgencies seek to carve out, administer, and govern "liberated areas," they are intimately connected to specific locales and populations in those locales. Because networked insurgencies do not seek or are unable to develop liberated areas which they administer and govern, they are less intimately linked to specific locales and populations. They can shift their area of operations to different parts of a country or even to other countries with little effort.

There are a number of things that make networked insurgencies prevalent in the contemporary security environment. One is the increased effectiveness of state security services. Proto-state insurgencies, particularly in their early stages, required ungoverned or poorly governed regions in which to establish their state-like organizations, including their guerrilla and, in some cases, conventional military capability. They needed the state to be unaware of their existence or at least to not take them seriously during their gestation period. Today, both the field of vision and operational effectiveness of state militaries make this difficult (but not impossible) to attain. The second reason is the decline in the use of insurgents as proxies. During the Cold War, the Soviet Union and, to a lesser extent, China, funded, equipped, trained, and supported insurgents as a method of indirect aggression against the West. This aided insurgent organizations in addressing the asymmetry between themselves and the state they sought to replace, making the proto-state model feasible. Today, external support for insurgencies still occurs but at a much lower level than

during the Cold War, making the proto-state model infeasible in the majority of cases. Even insurgents who would like to emulate Mao or Ho simply are unable to do so, and thus gravitate to other forms of insurgency. The third factor supporting networked insurgencies in today's strategic environment is the number of new technologies and systems for utilizing them—particularly the Internet and new media—that have made the dispersed, networked, transnational, and terrorism-focused organizations more effective and survivable and, therefore, more prevalent.

Insurgent Use of the Internet and New Media

When discussing the use of the Internet and new media by insurgents, we are actually discussing three separate but closely linked items: technology, systems for utilizing this technology, and a culture that influences how technology and systems operate. All are well known to anyone living in a moderately advanced nation or city around the world.

Foremost among the technologies is the Internet which is simply a system of devices and technologies used to exchange digital information. The second key technology is mobile communications which permit the exchange of information to take place.[3] The third are technologies to digitize data so it can be exchanged, particularly digital still and video cameras, along with the software to capture, alter, and share high quality images and video. This technology is now quite cheap, easy to acquire, and relatively easy to use. Until recently the technology to create high quality images and video was expensive and extremely complicated, thus limiting the number of users who could master it. It required extensive training. Since those individuals and organizations with the resources to purchase this expensive equipment and undergo the training to utilize it were relatively few, states knew who they were and often could control them. Today, images and videos are created and distributed via "decentralized networks of users who can incrementally improve (them) by applying personalized skill sets."[4] The old, industrial method of production required training workers who then built to standards under the supervision of a hierarchy. Distribution was executed in a similar manner. The new technique is "crowd sourcing," a collective process where self-inspired and often self-trained participants are involved, and quality control is via collective evaluations (commonly known as the "wiki" process after the Internet encyclopedia Wikipedia). In the broadest sense, the initial costs associated with being an information creator—whether it involves education, research, or physical equipment—are significantly lower than in the past, permitting more people, some with nefarious intention, to assume the role.

The system for the exploitation of new technology includes the World Wide Web, e-mail, file-sharing programs such as peer-to-peer networks, chat rooms, blogs, microblogs (most famously Twitter), instant messaging, short message services on mobile phones, social networking (most famously Facebook, but including thousands of other forms), cloud file storage and sharing

like Drop Box and Google Documents, photo sharing web sites such as Flickr and Photobucket, and video sharing such as YouTube and Google Videos.

The third component—and the one which makes the Internet and new media useful to insurgents—is the culture that supports its use. Technology itself did not create the culture, but it amplifies various trends, characteristics, and aspects. One important dimension of this is antiauthoritarianism. Young people, who are the most likely to embrace the Internet and new media, are naturally antiauthoritarian, particularly at this time in history when traditional structures for the exercise of authority have broken down. The Internet and social media add to this environment by allowing those with antiauthoritarian feelings to communicate with others who share their beliefs, capitalizing on what Audrey Cronin calls "a global explosion in chaotic connectivity."[5] Digital connection reinforces antiauthoritarian attitudes because those who hold these beliefs do not feel they are alone. In a broad sense, the world is witness to "the emergence of a visually-oriented, ideologically impulsive Internet culture with the means to rapidly and collectively plan and act."[6] In some societies this can lead to the development of the transnational hacker or hacktivist communities but it can also, with proper leadership, lead to the establishment of insurgent organizations. Phrased differently, it provides the psychological and attitudinal raw material for insurgents to exploit.

The Internet helps fill the authority vacuum left by the decline of traditional structures and the inability of the state to replace them. The challenge for twentieth century insurgents was to overcome the passivity and deference to authority among the peasantry, to stir them to action by overcoming the belief that they owed an obligation to the state but the state did not owe one to them. Today's insurgents do not face passivity and deference. Web-skilled youth inherently believe that the state has an obligation to them, to include the provision of services, education, and employment. The challenge for insurgents then is to organize, operationalize, and sustain the preexisting antiauthoritarianism. It is a matter of channeling an existing propensity to action rather than creating it. This is an important concept since much of the thinking regarding counterinsurgency is based on traditional and increasingly obsolete notions of authority as portrayed in the concept of legitimacy, which is often defined as an attribute of the state.

The culture of the Internet is depersonalizing and insurgents can exploit this fact. Organized violence always requires depersonalizing the enemy in an effort to overcome the natural reluctance to kill. The inherent depersonalization of the Internet facilitates this. Video games may contribute as well, making violence seem unreal and camouflaging its real cost. For many terrorists, their victims are simply characters in a game rather than real, living beings.

This blurring of the distinction between reality and a virtual world is a central component of Internet culture. For some who are immersed in this culture, it is difficult to distinguish their online, virtual life from their real one. In extreme cases, the virtual life dominates. Insurgents who use the Internet and social media for recruitment often exploit this phenomenon, portraying

an idealized, alternative reality imbued with moral clarity in a grand struggle between good and evil. This appeals to those lost in a depersonalized, virtual world. And just as there are no real costs for failing in a video game, these recruits can convince themselves that there are few or no personal costs for undertaking violence, whether it is mass murder or some other form of terrorism. The fact that it is easier to recruit terrorists who will complete a mission before reality of the act sets in and, therefore, only need a brief period of intense commitment rather than the extended commitment of a guerrilla, forces the modern insurgent to rely on terrorism as the preferred form of conflict. Terrorist recruits perform their acts before the commitment erodes. Terrorism is not necessarily more effective than guerrilla operations, but it is easier to create and sustain in the contemporary security environment.

It takes a special person to become an insurgent, to undertake the personal danger and hardship it entails. For traditional insurgents, finding those rare people was difficult. Because they make it easy, cheap, and safe to initiate contact with a large number of people, the Internet and new media greatly increase the ability of insurgents to find the type of recruits they are seeking. Once potential recruits express an interest in chat rooms, discussion boards, or by e-mail, insurgents can screen them and begin the recruitment process and integration into the movement.

The culture of the Internet and new media are also changing the traditional notion of credibility. For much of human history (and still in a number of societies), credibility is determined by affinity. The more affinity between the audience and the source of information—friends, family, clan, tribe, sect, religion, race, ethnicity—the greater the credibility of the information. As US forces in Iraq discovered, empirical evidence was less important than affinity in shaping an explanation of an event. In the modern age, credibility also derived from the authority of the source. Certain institutions are considered credible, normally because of the procedures they use to derive information and positions (fact checking, peer review, due process, etc.), because they represented traditional authority (monarchy, church) or because of the personality of the individual who represented that authority.

On the Internet, information and ideas move with such rapidity and in such complex ways, it is impossible to identify or gauge the authority of a given source. Information may have been passed through hundreds, thousands, or even millions of individuals and locations via e-mail, online discussions, blogs, web pages, tweets, and so forth. No one will be able to identify its origin. The criterion for credibility thus becomes the inherent receptivity of the receiver. People assign credibility to information or positions that reinforce their existing beliefs, in most cases, because they cannot gauge the authoritative nature of the original source. Anyone who has engaged in political debate sees this—for many people pointing to a web page that supports their position is validation enough. The Internet and new media are rife with myths which sometimes subside and then reappear at unpredictable times. No idea, no matter how delusional, suffers a final death in the virtual world. This aspect of Internet and new

media culture is a boon for insurgents, especially in societies with a proclivity to believe anything that portrays the state as repressive, nefarious, corrupt, evil, or inept. And these are precisely the sort of places where insurgency takes root.[7] Because the original source of the information is not known, audiences assign it credibility based on their general attitude regarding the state. When this attitude is negative, negative information becomes inherently credible.

Since one of the defining features of insurgency is the desire to center the struggle in the psychological realm where any material weakness of the insurgency is less debilitating than if it were in the conventional military realm; the culture of the Internet and new media afford insurgents great opportunity. Insurgents utilize specific technologies based on their perceived usefulness, its ease of use, and the risk involved.[8] Part of the appeal of the Internet and new media for insurgents is the low cost and lack of barriers to its use—any number of potential recruits already possess the technology and know how to use it.[9] The extensive numbers of people in cyberspace and virtual worlds also provide a degree of security. This is particularly important during the early, vulnerable stages of an insurgency. (Not unlike animals, most insurgencies die in childhood). By using the Internet and new media, nascent insurgencies reach widely dispersed audiences of potential recruits, supporters, and allies at a very low cost, and with less chance of discovery. As Brian Petit phrased it, "borderless social mobilization allows like-minded groups to coalesce digitally with less risk than the traditional early, vulnerable stages of building a resistance movement."[10] Given the huge amount of digital information constantly flowing, it is difficult for security forces to distinguish between serious threats and trivial ones. This lack of clarity affords insurgents a degree of protection. They may not be "amongst the people" but they are within the matrix.

The early stages of most insurgencies involve as great an internal struggle as an external one. Various factions and cliques compete for power and engage in conflict with each other.[11] The Internet provides a venue for such conflict, permitting factions and cliques to "conduct ideological debates or even personal disputes."[12] While crafting a coherent movement, insurgents no longer need a sanctuary where they can iron out their differences as the Bolsheviks and Mensheviks did in London and Switzerland, or the Vietnamese communists did in Paris and Moscow. In fact, Cori Dauber calls the Internet "the new Afghanistan" for violent extremists.[13] Internet-powered insurgencies can draw recruits and support from around the world, particularly if the instigators use transnational ideologies rather than purely local or nationalistic ones. The only prerequisites are Internet access and emotion. Both are abundant in today's uncertain strategic environment.

In addition to organization-forming and network building, insurgents find the Internet and new media useful for fundraising.[14] This is critical given the decline in (although not the end of) state sponsorship for insurgencies. Fundraising may take the form of soliciting donations from sympathizers or diasporas or, increasingly (as state security services pressure donators), involvement in online crime such as credit card fraud, identity theft, and other scams.

The Internet and new media also provide insurgents with a greatly expanded and more secure capacity for training, operational planning, and intelligence gathering. As Timothy Thomas notes, it provides "anonymity, command and control resources, and a host of other measures to coordinate and integrate attack options."[15] Iraqi insurgents, for instance, used Google Earth to identify targets and infiltration/exfiltration routes.[16] Other violent groups have found target maps, diagrams, and images online.[17] The relatively low cost, ease, and safety of online training and planning guides the insurgent toward an increased reliance on terrorism mainly due to its inherent ease of organization online when compared with a guerrilla operation. This is particularly true if the terrorist is deemed expendable. An organization minimizes the training it expends on an individual who will only perform one mission. These individuals normally do not want or need extensive, person-to-person contact or bonding. Online training is depersonalized, cheap, and easy. It becomes relatively painless for insurgent leaders to send individuals they have not met on a suicide mission. Hence, insurgencies are becoming terrorism-focused not because this is a particularly effective way of attaining their strategic objectives, but because the resources available lend themselves to such a strategy.

Effects Impacting the Insurgent's Use of Internet and New Media

What, then, does all this mean? In the broadest sense, the extensive use of or reliance on the Internet and new media drive insurgencies toward the adoption of a dispersed, networked, transnational, terrorism-centric movement, one that relies heavily on swarming tactics and operations. This type of insurgency has probably existed throughout history but only now does it have the tools to be effective. The Internet and new media allow such insurgencies to be acceptably effective at the three core functions of survival, strengthening itself, and weakening its enemy. With regard to networks in general, Arquilla and Ronfeldt note, "To realize its potential, a fully interconnected network requires a capacity for casting dense information and communications flows, more so than do other forms of organization."[18] Today's technology is capable of supporting an ever-expanding information flow. It has also reduced transmission times and cost, allowing dispersed units or organizations to communicate, coordinate, and swarm, either to targets or to successful narratives.[19] By acting with some degree of effectiveness even without central command and control, insurgencies as a movement are more survivable because they are not vulnerable to decapitation of their leadership. The destruction of any one node or even a small number of nodes in the organization is not debilitating.

The Internet and new media allow insurgencies to broaden their base by aggregating anger, frustration, and resentment inherent in many societies. Twentieth century insurgencies became powerful by aggregating local grievances which were always present in these societies. They did so by using face-to-face or traditional communication processes (writing, radio, etc.). These types of activities served as a constraint since potential supporters had to be contacted in person. The Internet and new media make it easy and cost

effective to contact a much larger group of angry, frustrated, resentful individuals. While the proportion of these supporters who are moved to action may be small, the large number of individuals contacted means that the aggregate size of the force that is moved to action can be significant. This is the same strategy behind e-mail spam or scams: even though the number of recipients who respond in some manner may be small, the fact that the spammers and scammers contact thousands or millions of individuals at a low cost makes the enterprise worthwhile. The Internet and new media are particularly useful for insurgent leaders during major strategic shifts within the movement such as the creation of an insurrection that will serve as a precursor or catalyst for the insurgency, the transformation from insurrection into sustainable insurgency, or when initiating efforts to regain the strategic initiative or stave off some impending threat.

Mobilization based on the Internet and new media is often fueled by raw anger and resentment more than a specific and complex ideology—it has broad appeal. These emotions can give insurgents the ability to surge. When facing an unpopular regime, they can rapidly mobilize an extensive opposition with the hope of overloading the regime's response capability while goading it into a major mistake. Such an emotional response does not, however, automatically guarantee the beginning of an insurgency. The case of Iran suggests that a brutal and effective regime may quash an insurrection before it becomes an insurgency. Egypt and Tunisia, likewise, suggest that fragile regimes may collapse rather quickly, making insurgency unnecessary. But Libya and Syria suggest that once an insurrection is mobilized, at least partially, by the Internet and new media, it has the potential for developing into a full-scale insurgency. The more dependent a regime is on outside support that can be manipulated via the Internet and social media, the more critical these capabilities become to the insurgents. Of course, the more pervasive the Internet and social media in a particular nation, the greater the chances are that the insurgents will utilize them. Egypt and Tunisia were more vulnerable to Internet and new media opposition because their former regimes were more dependent on external support than the regimes of Iran, Libya, or Syria.

Once an information-rich insurrection is transformed into an insurgency, the multiplicity of connections and communications among individuals and groups makes it difficult to control and predict the effect of a given narrative. This makes the psychological domain of insurgency, which is always critical, much more complex than in the past. The days when insurgents or counterinsurgents could identify a handful of key themes and simply promulgate them in word and deed are long past. Because it is so much easier to communicate with any number of audiences, it becomes harder to gauge the impact of that communication, causing insurgents to craft multiple, even conflicting narratives. When one or more of these initiatives appear to be having some desired effect, the insurgents can reinforce and amplify them. This is not linear strategy in the traditional sense of predicting the most effective way of

attaining a desired end, but a strategy of complexity based on trying numerous activities simultaneously to see which ones work.

A strategy of complexity allows purposeful (but not strategic) action by networks comprised of diverse nodes that are often motivated by subideological factors such as anger or frustration. Internet and new media-based insurgencies do not need (and cannot attain) unity of purpose, but only unity of action. As Marc Sageman notes, "The mass nature of Internet communications encourages sound bites and reductionist answers to difficult questions. Drawn to their logical conclusions, these views encourage extreme, abstract, but simplistic solutions without regard to the reality and complexity of life."[20]

The use of the Internet and new media by insurgents can be depicted as a continuum: at one end are the traditional insurgencies which simply use these capabilities as a force multiplier. For example, the Taliban is beginning to make greater use of information technology. Younger, technology-savvy insurgents use laptop computers, mobile phones, digital cameras, and global positioning system (GPS) devices for urban reconnaissance, often driving around Afghan cities with dashboard-mounted webcams.[21] These videos are then used for targeting and operational planning. At the other end of the spectrum would be insurgencies created with the Internet and new media relying almost exclusively on the terrorism-focused, swarming methods derived from the utilization of these capabilities. Almost all twenty-first century insurgencies fall somewhere on this spectrum.

Conclusions

The prevalence of dispersed, networked, transnational, terrorism-centric insurgencies relying heavily on swarming tactics and operations is both bad and good news. The bad news is that such organizations are extremely difficult to defeat and eradicate. The Internet and new media cannot be quashed and it is impossible to fully overcome anger and frustration, particularly among the younger population. Because they are networked and transnational, these insurgencies can survive the destruction of a large number of their nodes. Like an Internet myth, they may appear to be dead only to reappear at some unpredictable place or time. Ultimately they cannot be defeated, only managed. Even if it made sense to approach twentieth century counterinsurgency as a form of warfare with the objective of a decisive victory, it makes no sense to approach twenty-first century ones in that manner. "Victory" over twenty-first century insurgents will be as meaningless as victory over the phenomenon of criminal gangs. If one gang is beaten into submission, it normally reemerges in a similar or even identical form, largely due to the fact it is impossible or exorbitantly expensive to alter the social, political, cultural, and economic system that spawned them initially.

The good news is that dispersed, networked, transnational, terrorism-centric insurgencies utilizing swarming tactics and operations are unlikely to attain any decisive victory. This type of organization is much more likely to suffer decisive defeat, at least if it does not have major outside support. They

simply cannot mobilize, focus, and control sufficient power to overcome a state that is capable of sustaining its morale and coherence. Again, a major exception to this relationship may be a state dependent on outside support. If a networked insurgency can erode such support, the state will, in all likelihood, fail (though the insurgents are then likely to lapse into internecine conflict since, in most cases, unlike the Maoist insurgents of the twentieth century, they are not structured to assume the power and functions of the state). Perhaps the most prevalent model for these groups will be Internet and new media-driven, nonviolent insurrections struggling against states that are dependent on outside support, such as Egypt and Tunisia. It is not clear whether these insurrections would have mutated into actual insurgencies had the Egyptian and Tunisian governments fought back.

Insurgents inevitably emulate success. In the twentieth century, when the proto-state Maoist approach was successful, others emulated it. Some succeeded, some did not. Today, insurgents and potential insurgents continue to copy each other. The challenge for the United States, particularly the Army, is to develop counterinsurgency concepts, doctrine, organizations, and leaders which are capable of countering the ongoing variegation of insurgency. The "one size fits all" concept has to be abandoned, whether it applies to a particular form of insurgency, one that treats Maoist insurgencies as a universal model, or of a counterinsurgency, the idea that protecting the population and strengthening the state are the keys to success. Ultimately dispersed, networked, transnational, terrorism-centric insurgencies can only be managed, not defeated, in the traditional sense of the word. Programs for dealing with criminal gangs may provide a better analogy than warfighting, which provided the base line for the original US counterinsurgency strategy and doctrine in the mid-twentieth century. The sooner America's Army and the rest of the US government accept this, the better they will be at countering these challenging foes.

Notes

1. Thinking on this is detailed in Steven Metz, "Rethinking Insurgency," in *The Routledge Companion to Insurgency and Counter Insurgency*, ed. Paul Rich and Isabelle Duyvesteyn (London: Routledge, 2012); and Steven Metz, "Insurgency," in *Conceptualising Modern War: A Critical Inquiry* , eds. Ole Jørgen Maaø and Karl Erik Haug (London: Hurst, 2011).

2. The concept of commercial insurgency is introduced Steven Metz, *The Future of Insurgency* (Carlisle Barracks, PA: United States Army War College Strategic Studies Institute, 1993). It has been revived, largely because of the conflict in Mexico. For example, Volume 22, no. 5, of the journal *Small Wars and Insurgencies* dealt with what the editors called "Criminal Insurgencies in Mexico and the Americas: The Gangs and Cartels Wage War."

3. The parts of the world without cell phone coverage are shrinking daily. Even large sections of the most backward parts of the world like Somalia have service.

4. John Curtis Amble, "Combating Terrorism in the New Media Environment," *Studies in Conflict and Terrorism* 35, no. 5 (May 2012): 342.

5. Audrey Kurth Cronin, "Cyber-Mobilization: The New *Levee en Masse*," *Parameters* 36, no. 2 (Summer 2006): 82.

6. Brian Petit, "Social Media and UW," *Special Warfare* 25, no. 2 (April-June 2012): 26.

7. The tendency to consider anything that casts the state in a negative light is certainly not limited to the sort of states prone to insurgency—it exists just as much in the United States as anywhere

8. Bruce Forrester, Anissa Frini, and Régine Lecoq, "Understanding the Role of Social Media in a Counter-Insurgency Context," *NATO Research and Technology Organization Information Systems Technology Symposium* (Madrid, Spain: May 9-10, 2011), 14.

9. Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Washington, DC: United States Institute of Peace, 2006), 30.

10. Petit, "Media and UW," 25.

11. Much analysis of insurgency underestimates this because it focuses on mature, late-stage insurgencies.

12. Weimann, *Terror on the Internet*, 141.

13. Cori E. Dauber, *YouTube War: Fighting in a World of Cameras in Every Cell Phone and Photoshop on Every Computer* (Carlisle Barracks, PA: United States Army War College Strategic Studies Institute, 2009), 29.

14. See Weimann, *Terror on the Internet*, 134-141; Timothy L. Thomas, "Al Qaeda and the Internet: The Danger of 'Cyberplanning'," *Parameters* 33, no. 1 (Spring 2003): 116-117; and Michael Jacobson, "Terrorist Financing and the Internet," *Studies in Conflict and Terrorism* 33, no. 4 (2010): 353-363.

15. Thomas, "Al Qaeda and the Internet," 112.

16. Dauber, *YouTube War*, 16-17.

17. Weimann, *Terror on the Internet*, 111-114.

18. John Arquilla and David Ronfeldt, "The Advent of Netwar (Revisited)," in *Networks and Netwars* (Santa Monica: RAND Corporation, 2001), 10.

19. Michele Zanini and Sean J. S. Edwards, "The Networking of Terror in the Information Age," in *Networks and Netwars*, ed. John Arquilla and David Ronfeldt (Santa Monica, RAND Corporation, 2001), 35-36.

20. Marc Sageman, *Understanding Terror Networks* (Philadelphia: University of Pennsylvania Press, 2004), 162.

21. Ron Moreau and Sami Yousafzai, "Afghanistan: The Taliban's High-Tech Urban Strategy," *Newsweek*, May 28, 2012.